Raymond P. Boucher, State Bar No. 115364
ray@boucher.la
Shehnaz M. Bhujwala, State Bar No. 223484
bhujwala@boucher.la
Maria L. Weitz, State Bar No. 268100
weitz@boucher.la
BOUCHER LLP
21600 Oxnard Street, Suite 600
Woodland Hills, California 91367-4903
Tel: (818) 340-5400
Fax: (818) 340-5401

Attorneys for Plaintiffs Kelly Tharp, Daniel Tharp, and Kenneth Coonce

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, EASTERN DIVISION

KELLY THARP, Individually, and on Behalf of All Others Similarly Situated; DANIEL THARP, Individually, and on Behalf of All Others Similarly Situated; KENNETH COONCE, Individually, and on Behalf of All Others Similarly Situated, Plaintiffs, v. ANTHEM, INC., d/b/a ANTHEM HEALTH, INC., an Indiana Corporation; THE ANTHEM COMPANIES, INC., an Indiana Corporation; THE ANTHEM COMPANIES OF CALIFORNIA, INC., a California Corporation; ANTHEM BLUE CROSS LIFE AND HEALTH INSURANCE COMPANY, A California Corporation; and DOES 1-10, Inclusive, Defendants.	Case No. 5:15-cv-1046 CLASS ACTION **CLASS ACTION COMPLAINT** 1. Violations of California's Unfair Competition Law [Cal. Bus. & Prof. Code § 17200 *et seq*.]; 2. Violation of California's Data Breach Act [Cal. Civ. Code § 1798.80 *et seq*.]; 3. Violation of California's Confidentiality of Medical Information Act [Cal. Civ. Code § 56 *et seq*.] 4. Negligence **DEMAND FOR JURY TRIAL**

Plaintiffs Kelly Tharp, Daniel Tharp, and Kenneth Coonce, individually and on behalf of a class of all other similarly situated persons defined below ("Plaintiffs"), allege and complain the following facts and counts against defendants Anthem, Inc., doing business as Anthem Health, Inc., an Indiana corporation, The Anthem Companies, Inc., an Indiana corporation, The Anthem Companies Of California, Inc., a California corporation, Anthem Blue Cross Life And Health Insurance Company, a California corporation, and Does 1-10, inclusive ("Defendants"), and respectfully request a trial by jury of all issues and causes of action so triable.

INTRODUCTION

1. Plaintiffs bring this class action lawsuit on behalf of themselves and all other persons similarly situated, whose privacy rights Defendants violated and continue to violate, and whose security Defendants have placed at great risk.

2. Defendants uniformly failed to implement and maintain security measures and protocols to protect the personal information of current and former members of Defendants' affiliated health insurance plans, including their names, dates of birth, Social Security numbers, medical identification numbers, home addresses, e-mail addresses, employment information including income data, and possibly medical information, which Defendants maintained and/or stored on their databases and servers.

3. Defendants' policies and practices resulted in a massive data breach by third party hackers announced by Defendants on February 4, 2015, whereby the personal information of Plaintiffs and Class members was accessed and exposed. By Defendants' own estimate, 13.5 million Californians were affected by the data breach from the estimated 78.8 million persons affected nationwide.[1]

---

[1] 13.5 Million Californians Affected by Anthem Data Breach, LA Times (February 24, 2015): *www.latimes.com/business/la-fi-anthem-data-breach-20150224-*

4. Defendants failed to implement and maintain security measures to prevent this breach, to promptly detect this breach, and to render the accessed data containing the personal information of Plaintiffs and Class members unreadable through industry-standard encryption methods.

5. Defendants' policies and practices have caused and will continue to cause Plaintiffs and Class members to suffer identity theft or the significant risk thereof for years to come. Defendants' offer of two years of credit monitoring is not enough to compensate Plaintiffs and Class members, including minors, for the harms they have suffered and will continue to suffer in years to come.

PARTIES

6. Plaintiffs Kelly Tharp and Daniel Tharp are, and at all material times were, California citizens residing in the city of Hesperia, San Bernardino County, California. At all material times, the Tharps have been members of Defendants' Anthem Blue Cross health insurance plan offered through Daniel Tharp's work. Defendants obtained the Tharps' personal information including their names, dates of birth, Social Security numbers, medical identification numbers, home addresses, e-mail addresses, and employment information including income data, as a result of their membership in Defendants' plan. In early February, 2015, the Tharps learned of the Data Breach from news reports. In early April, 2015, the Tharps discovered that they were victims of identity theft when they learned someone had used their personal information to file a false tax return and started to receive calls from bill collectors about a debt they did not owe. Following this discovery, the Tharps contacted Defendants using the toll free number provided on Defendants' website, *www.anthemfacts.com*, but Defendants' representative would not confirm or deny whether their personal information was accessed in the breach. The Tharps have been forced to take measures to protect themselves and their credit from the identity

---

story.html.

theft, including freezing their credit for approximately $60, and have suffered harm and incurred damages as a direct and proximate result of Defendants' conduct alleged herein.

7. Plaintiff Kenneth Coonce is, and at all material times was, a California citizen residing in the city of Sanger, Fresno County, California. At all material times, Plaintiff Coonce has been a member of Defendants' Anthem Blue Cross health insurance plan offered through his work. Defendants obtained his personal information including his name, date of birth, Social Security number, medical identification number, home address, e-mail address, and employment information including income data, as a result of his membership in Defendants' plan. In early February, 2015, Plaintiff Coonce first learned of the Data Breach from news reports. Thereafter, he received a letter from Defendants dated March 19, 2015, notifying him in writing of the breach. Plaintiff Coonce has suffered harm and incurred damages as a direct and proximate result of Defendants' conduct alleged herein.

8. Defendant Anthem, Inc., which is doing business as Anthem Health, Inc. in California, is and at all material times was a corporation organized and existing under the laws of Indiana, with a principal place of business located at 120 Monument Circle, Indianapolis, Indiana, 46204. Anthem, Inc. is operating and conducting business under the laws of California and regularly conducts business throughout this District and Division. Prior to December 2014, Anthem, Inc. was known as Wellpoint, Inc., one of the largest health insurance companies in the United States.

9. Defendant The Anthem Companies, Inc. is and at all material times was a corporation organized and existing under the laws of Indiana, with a principal place of business located at 120 Monument Circle, Indianapolis, Indiana, 46204. The Anthem Companies, Inc. is operating and conducting business under the laws of California and regularly conducts business throughout this District and Division.

10. Defendant The Anthem Companies of California, Inc., is and at all

material times was a corporation organized and existing under the laws of California, with a principal place of business located at 120 Monument Circle, Indianapolis, Indiana, 46204. The Anthem Companies of California, Inc. is operating and conducting business under the laws of California and regularly conducts business throughout this District and Division.

11. Defendant Anthem Blue Cross Life and Health Insurance Company is and at all material times was a corporation organized and existing under the laws of California, with a principal place of business located at 120 Monument Circle, Indianapolis, Indiana, 46204. Anthem Blue Cross Life and Health Insurance Company is operating and conducting business under the laws of California and regularly conducts business throughout this District and Division.

12. The Defendants sued by the fictitious names DOES 1 through 10 are persons or entities whose true names and identities are currently unknown to Plaintiffs. Plaintiffs will amend this Complaint to allege the true names and capacities of these fictitiously named Defendants when they are ascertained. Each of the fictitiously named Defendants is responsible for the conduct alleged in this Complaint. Through their conduct, the fictitiously named Defendants actually and proximately caused the damages of Plaintiffs and the Class.

13. In this Complaint, Defendants Anthem, Inc. d/b/a Anthem Health, Inc., The Anthem Companies, Inc., The Anthem Companies of California, Inc., Anthem Blue Cross Life and Health Insurance Company, and Does 1 through 10, inclusive, are sometimes referred to individually as “Defendant” or by name, and are sometimes referred to collectively as “Defendants,” or “the Defendants.”

14. At all times mentioned herein, each Defendant was acting as the agent and/or employee of each of the remaining Defendants and was at all times acting within the purpose and scope of such agency and employment. In doing the acts alleged herein, each Defendant, and its officers, directors, members, owners, principals, or managing agents (where the defendant is a corporation, limited

liability company, or other form of business entity) authorized and/or ratified the conduct of each other Defendant and/or of his/her/its employees.

JURISDICTION AND VENUE

15. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which (i) the proposed class consists of more than 100 members; (ii) at least some members of the proposed class and/or subclass are citizens of a state different from at least one of the defendants; and (iii) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over Defendants because they are authorized to conduct business in California, have sufficient minimum contacts in California, or otherwise intentionally avail themselves of the markets within California, through the marketing and sale of health insurance plans in California.

17. Venue is proper in the Central District of California, Eastern Division, pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events that give rise to the claims herein occurred in this District. In particular, the Tharps' purchase and use of Defendants' Anthem Blue Cross health insurance plan took place within this District and Division. Venue is also proper because Defendants transact substantial business in this District and Division.

18. All of the allegations contained in this Complaint are based upon information and belief, except for those pertaining to Plaintiffs and their counsel. Plaintiffs' information and belief are based upon, among other things, the investigation that Plaintiffs and their counsel have conducted to date. The allegations in this Complaint are substantiated by evidentiary support or are likely to be substantiated by evidentiary support upon further investigation and discovery.

FACTUAL BACKGROUND

A. Anthem Data Breach

19. On February 4, 2015, Defendants announced that hackers had gained

access to Defendants' databases and obtained personal information of current and former members, such as their name, date of birth, Social Security number, medical identification number, home address, e-mail address, and employment information including income data.[2] To date, Defendants have not clearly stated whether financial or medical information was accessed or disclosed as a result of the breach, stating instead that there is no evidence of that such information was targeted or compromised based on what Defendants currently know. The accessed database contained records for up to 80 million customers.[3] As stated previously, by Defendants' own estimate, approximately 13.5 million Californians were affected by the data breach.

20. According to Defendants' website, *www.anthemfacts.com*, Defendants discovered the breach on January 29, 2015. Defendants state that "cyberattackers tried to get private information about current and former Anthem members ….over the course of several weeks beginning in early December, 2014."[4] However, the breach may have started as far back as April, 2014, nine months before Defendants indicate they discovered the breach.[5]

21. Defendants state on their website that all product lines were impacted by the breach, "except for those current or former Anthem members who only had coverage for workers compensation, life or disability insurance only."[6] The impacted (plan/brand) include Anthem Blue Cross, Anthem Blue Cross and Blue

---

[2] *See* Letter from Joseph R. Swedish, President and CEO Anthem, Inc.: *www.anthemfacts.com/ceo*.

[3] *See* Health Insurer Anthem Hit by Hackers, Wall Street Journal (February 4, 2015): *www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720*.

[4] *See* Letter to Members dated February 13, 2015: *www.anthemfacts.com/*.

[5] *See* Anthem Data Breach May Have Started in April 2014, Krebs on Security article dated February 15, 2015: *krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/*.

[6] *See* Frequently Asked Questions*: www.anthemfacts.com/faq*.

Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, HealthKeepers and Golden West.[7]

22. While Defendants maintain they were the target of "a very sophisticated external cyber attack" whereby "attackers gained unauthorized access to Anthem's IT system,"[8] news reports and security-focused online blogs suggest otherwise. Indeed, the breach was discovered when a database administrator reportedly discovered that his system log in credentials were being used to perform a query he did not initiate on or about January 27, 2015.[9] The credentials of as many as five of Defendant' employees were compromised possibly through relatively simple phishing efforts and consistent measures to access the system.[10]

23. While Defendants' President and CEO assures customers that safeguarding their personal, financial and medical information is a top priority, and that Defendants maintain "state-of-the-art information security systems" to protect customer data,[11] Defendants failed to implement and maintain at least a two-factor authentication (2FA) process for all employees that could have prevented the breach or detected the same much earlier, despite the compromise of employee log in credentials.[12][13][14] The sensitive data of Defendants' customers was secured only by a

---

[7] *Id.*

[8] *See*: *www.anthemfacts.com/ceo*.

[9] *See* Anthem: How Does a Breach Like This Happen?, CSO (February 9, 2015): *www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html.*

[10] *Id.*

[11] *See www.anthemfacts.com/ceo*.

[12] *See* Health Records Are the New Credit Cards, Threat Connect (March 19, 2015): *www.threatconnect.com/news/news-articles/march-19-cso-online-health-records-are-the-new-credit-cards/.*

[13] *See* An Anthem to Get Behind: Enable Two-Factor Authentication, RSAConference (February 17, 2015): *www.rsaconference.com/blogs/an-anthem-to-*

log in and password, not a second or even third layer of protection such as a card, key fob, token or application that generates a temporary password.[15] Defendants also failed to maintain monitoring technology sensitive enough to detect unusual queries or transfer of data, and failed to encrypt the entire database.[16]

B. Defendants' Misrepresentations Regarding Compliance and Safety

24. At all relevant times, Defendants have mislead (and continue to mislead) the public concerning the safety of its privacy practices.

25. For example, Defendants' Anthem Blue Cross Life and Health Insurance policy materials as of April 2010 state: "Because PI is defined as any information that can be used to make judgments about your health, finances, character, habits, hobbies, reputation, career and credit, we take reasonable safety measures to protect the PI we have about you."

26. The same policy materials go on to represent:

> We are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure. We keep your oral, written and electronic PHI safe using physical, electronic, and procedural means. These safeguards follow federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password protecting computers, and locking storage areas and filing cabinets. We require our employees to protect PHI through written policies and procedures. These policies limit access to PHI to only those employees who need the data to do their job. Employees are also required to wear ID badges to help keep people who do not belong out of areas where sensitive data is kept. Also, where required by law, our affiliates and nonaffiliates must protect the privacy of data we share in the normal course of business. They are not allowed to give PHI to others without your written OK, except as allowed by law.

27. These types of promises create duties on behalf of Defendants to secure

---

get-behind-enable-two-factor-authentication.

[14] *See* Anthem's IT System Had Cracks Before Hack, Indianapolis Business Journal (February 14, 2015): *www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack.*

[15] *Id.*

[16] *Id.*

the personal information of members and former members of Defendants' affiliated health insurance plans in accordance with the same (or greater) standards promised with the latest security best practices and trends and require Defendants to continue to build security into the services it offers. In addition to its contractual duties, Defendants owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard its customers' personal information.

28. Defendants cannot disclaim or limit their liability for their security breaches and violations of law because any such purported terms or waivers in policies or contracts are contrary to well established public policy are unenforceable under California law.

C. The Impact of Defendants' Actions on Consumers

29. The impact of Defendants' sub-standard security practices on their current and former members is far-reaching. Paul Stephens, director of policy and advocacy at the Privacy Rights Clearinghouse, posits that access could be gained by criminals to existing financial or consumer accounts with the personal information of Plaintiffs and Class members that Defendants failed to reasonably protect.[17] Moreover, new accounts may be opened with such information unless extreme measures such as security freezes are taken, which option remains unavailable for minors in many states, including California. Additionally, Plaintiffs and Class members are at greater risk to phishing attacks wherein additional personal information such as account names and passwords for online accounts are obtained. And, as was the experience of the Tharps, the theft of Social Security numbers heightens the risk of tax fraud, where stolen personal information is used to claim tax refunds.

---

[17] Protecting Yourself from the Consequences of Anthem's Data Breach, New York Times (February 5, 2015): *www.nytimes.com/2015/02/06/business/protecting-yourself-from-the-consequences-of-anthems-data-breach.html*.

30. As a result of Defendants' security policies and practices, Plaintiffs and Class members have incurred or are at risk of incurring varied damages, such as bank fees for obtaining new credit and debit cards, overdraft charges, costs arising from the inability to use or access financial accounts such as the inability to pay other bills, costs associated with credit-related services such as credit monitoring, detecting, or freezing, costs associated with false or fraudulent charges on credit or debit accounts, costs associated with false or fraudulent tax returns, not to mention the time and effort lost from dealing with identity theft or mitigation efforts.

31. In short, Defendants' failure to maintain appropriate security measures for its systems have left the privacy and security of millions of consumers vulnerable in ways that cannot be remedied by programs that simply monitor members' credit and bank accounts for fraudulent activity. Until Defendants adopt appropriate, industry-compliant security measures, Plaintiffs and Class members will remain at risk.

CLASS ACTION ALLEGATIONS

32. Plaintiffs bring this action on behalf of themselves and all others similarly situated as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure. This action may be brought and properly maintained as a class action because Plaintiffs satisfy the numerosity, adequacy, typicality, and commonality pre-requisites for suing as representative parties pursuant to Rule 23.

33. **Class Definition**. The proposed plaintiff Class that Plaintiffs seek to represent is preliminarily composed of and defined as follows:

> All current and former members of Defendants' affiliated health insurance plans in California whose personal information was compromised as a result of the data breach announced on February 4, 2015 ("Class").

34. Excluded from the Class are Defendants named herein; officers and directors of Defendants; members of the immediate family of any Defendant; any judges or justices to whom this action is assigned and their immediate families; and

the legal representatives, heirs, successors, or assigns of any such excluded party.

35. Plaintiffs reserve the right to amend or otherwise alter the Class definition presented to the Court at the appropriate time, or propose or eliminate sub-classes, in response to facts learned through discovery, legal arguments advanced by Defendants, or otherwise.

36. **Numerosity and Ascertainability**. The members of the Class are so numerous that joinder of all members is impracticable. By Defendants' own estimate, the current and former members in California whose personal information was compromised as a result of the breach is estimated by Defendants to be 13.5 million individuals. Moreover, the precise number of Class members and their addresses may be obtained from a review of Defendants' own records and/or records in the control of Defendants. This information may then be used to contact potential Class members.

37. **Typicality**. Plaintiffs are members of the Class. Their claims are typical of the claims of other members of the Class they seek to represent. The harm that Plaintiffs and all other Class members suffered arose from, and was caused by, the same conduct by Defendants. Defendants have acted, or refused to act, on grounds generally applicable to the Class, thereby making injunctive relief and damages appropriate with respect to the Class as a whole.

38. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class members. Plaintiffs have retained counsel that is competent and experienced in consumer class action litigation to ensure such protection. Plaintiffs and their counsel intend to prosecute this action vigorously for the benefit of the Class. Plaintiffs have no interests that are antagonistic to those of the Class. Plaintiffs have no interests that are in conflict with those of the Class.

39. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy for several reasons. First, the

damages suffered by each Class member are too small to warrant individual pursuit and thus a class action is the only viable method to obtain damages and other relief from Defendants. Second, class treatment would be superior to adjudicating individual cases due to the much greater expense and burden that individual litigation would impose upon the courts. Third, if Class members sought relief through individual actions, inconsistent or varying adjudications in their individual cases could establish incompatible standards of conduct for the Defendants.

40. **Predominance of Common Questions of Law and Fact**. There exists a well-defined community of interest in the questions of law and fact involved in this case against Defendants, and in obtaining appropriate relief for Defendants' violations of Plaintiffs' and Class members' rights under statutes and common law. Pursuant to Rule 23(b)(3), the following questions of law and fact common to the Class predominate over any individualized issues and the answers to these questions are apt to drive the resolution of the litigation:

a. Whether Defendants' actions as alleged herein violated California's Unfair Competition Act;

b. Whether Defendants' actions constitute a violation of the California Data Breach Act (Cal. Civ. Code § 1798.90 *et seq*.);

c. Whether Defendants' acts and omissions constitute a violation of the California Online Privacy Protection Act (Cal. Bus. & Prof. Code § 22576);

d. Whether Defendants' actions violated the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56 *et seq.*)

e. Whether Defendants' actions as alleged herein constitute negligence under common law;

f. Whether Plaintiffs and Class members are entitled to recover damages as a result of Defendants' violations of their rights under statutory and common laws as alleged herein; and

g. Whether Plaintiffs and Class members are entitled to injunctive relief to enjoin or restrain the Defendants from committing further violations of consumer rights under statutory and common laws.

41. The core factual and legal issues are the same for all Class members: (a) whether the Class member is a current or former member of one of Defendants' affiliated health insurance plans in California; (b) whether the Class member's personal information was compromised as a result of the data breach announced on February 4, 2015; (c) the harm Plaintiffs and Class members suffered thereby; and (d) the measure of damages and injunctive relief that are deemed appropriate.

42. The proposed Class may also be certified under Rule 23(b)(1) or (b)(2) because: (a) the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants; (b) the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and (c) Defendants have acted or refused to act on grounds that apply generally to the proposed class, thereby making appropriate final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

43. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT ONE

FRAUDULENT, UNFAIR, AND UNLAWFUL BUSINESS PRACTICES

[Bus. & Prof. Code § 17200 *et seq.*]

(Against All Defendants)

44. Plaintiffs incorporate by reference the allegations in all preceding paragraphs of this Complaint as though fully set forth herein.

45. Defendants' business practices, as alleged herein, are unfair within the meaning of Business and Professions Code section 17200 *et seq*. as the harm caused to the public as a result of Defendants' practices far outweighs any benefit conferred thereby.

46. Defendants' business practices, as alleged herein, are unlawful within the meaning of Business and Professions Code section 17200 *et seq*. as they constitute violations of California Civil Code section 1798.90 *et seq*. ("California Data Breach Act"), Business & Professions Code section 22576 ("California Online Privacy Protection Act"), and California Civil Code section 56 *et seq*. ("California Confidentiality of Medical Information Act").

47. As a direct and proximate result of Defendants' above-mentioned conduct, each member of the proposed Class suffered monetary injury in amounts unjustly collected from Class members. Plaintiffs and the Class members are entitled to restitution of such monies in amounts to be established by proof at trial.

48. Moreover, Defendants continue to engage in the above-described practices and unless enjoined from doing so by this Court, will continue to do so, all to the damage of current and former members on the basis of their deceptive and unlawful practices.

COUNT TWO

VIOLATION OF CALIFORNIA'S DATA BREACH ACT

[Cal. Civ. Code § 1798.80 *et seq*.]

(Against All Defendants)

49. Plaintiffs incorporate by reference the allegations in all preceding paragraphs of this Complaint as though fully set forth herein.

50. The California Data Breach Act ("CDBA") creates a duty for businesses that maintain computerized databases containing personal information to notify affected PERSONS "of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to

have been, acquired by an unauthorized person.” (Cal. Civ. Code § 1798.82.)

51. Defendants failed to inform all Class members about the security breach and compromise of their personal information within a reasonable amount of time after Defendants became aware the data breach had occurred.

52. Defendants unreasonably delayed disclosing the breach of security of Personal Information to Class members following discovery, despite knowing or reasonably believing that consumers’ personal information had been acquired by unauthorized persons.

53. Upon information and belief, Defendants were not instructed by any law enforcement agency to delay notification of the data breach to Plaintiffs and the other Class Members.

54. Pursuant to Civil Code section 1798.84:

> Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> …
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

55. As a result of Defendants’ violation of Civil Code section 1798.82, Plaintiffs and the other Class Members suffered monetary injury including improper disclosure of their Personal Information, loss of privacy, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud as a consequence

of the data breach, the value of their time spent mitigating identity theft, fraud, and/or the increased risk of identity theft and/or fraud, and deprivation of the value of their personal information, for which there is a well-established national and international market.

56. Plaintiffs seek all remedies available under the Data Breach Act, including, but not limited to actual damages, statutory damages for Defendants' willful, intentional, and/or reckless violation of California Civil Code section 1798.83, and equitable relief, as well as reasonable attorneys' fees and costs under Civil Code section 1798.84(g).

COUNT THREE

VIOLATION OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT

[Cal. Civ. Code § 56 e*t seq*.]

(Against All Defendants)

57. Plaintiffs incorporates by reference the allegations in all preceding paragraphs of this Complaint as though fully set forth herein.

58. California's Confidentiality of Medical Information Act, California Civil Code Sections 56 *et seq*. ("CMIA") requires health care providers who receive medical information of patients to establish procedures to ensure the confidentiality and protection from unauthorized use and disclosure of such information, including but not limited to security systems restricting access to files containing medical information. It also prohibits providers from disclosing medical information regarding a patient without written authorization.

59. Defendants are providers of health care within the meaning of Civil Code section 56.06(a). Plaintiffs are "patients" of Defendants, as defined in Civil Code section 56.06(h).) Defendants maintain medical information of the Plaintiffs as defined in Civil Code section 56.06(g).

60. Defendants maintained certain medical information and records

regarding Plaintiffs and Class members. Pursuant to the CMIA, Defendants had a legal duty to implement policies and practices to protect the confidentiality of such information and records.

61. Defendants breached their duty to Plaintiffs and Class members to protect the confidentiality of their medical records and information by failing to implement and maintain reasonable security measures to prevent unauthorized access to Defendants' systems and databases and disclosure of the same.

62. Pursuant to California Civil Code section 56.36, Plaintiffs and Class members whose medical information and records were accessed without authorization and/or disclosed are entitled to statutory damages of $1,000, in addition to any actual damages.

COUNT FOUR

NEGLIGENCE

(Against All Defendants)

63. Plaintiffs incorporate by reference the allegations in all preceding paragraphs of this Complaint as though fully set forth herein.

64. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in collecting, maintaining, storing, managing, retaining, securing, safeguarding, and/or deleting their personal information, such that it would be adequately protected from being accessed, compromised, stolen, misused, and/or disclosed, unauthorized persons disclosure and use.

65. The duty Defendants owed to Plaintiffs and Class members is underscored by California's Data Breach Act and CMIA, which laws were enacted to protect the privacy rights of consumers related to their confidential personal and medical information.

66. Defendants knew or should have known of the industry "best practices" for securing the personal information of Plaintiffs and Class members, but failed to follow them.

67. By Defendants' unlawful acts and omissions, Defendants breached their duty to Plaintiffs and Class members to use reasonable care to protect and adequately maintain their personal information. Defendants specifically failed to implement and maintain reasonable security measures to protect the personal information of Plaintiffs and Class members stored on their systems and databases from unauthorized access, use, and disclosure.

68. Defendants' negligence was a substantial factor in causing the harm suffered by Plaintiffs and Class members. As a proximate result of Defendants' breach of its duty, Plaintiffs and Class members suffered economic and other damages. Plaintiffs and Class members have and will be required to incur expenses in terms of time and money to attempt to protect themselves from identity theft, harm to their reputations and their credit.

69. Plaintiffs seeks damages in amounts to be determined at the time of trial, as well as injunctive relief, as a result.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for relief and judgment against Defendants, jointly and severally, as follows:

1. For an order certifying the proposed class and appointing Plaintiffs as Class representative and their counsel as Class Counsel;

2. For actual, compensatory and/or statutory damages;

3. For equitable relief enjoining Defendants from continuing to engage in the unlawful, unfair, and fraudulent business practices described in this Complaint;

4. For equitable relief requiring Defendants to make full restitution of all monies wrongfully obtained and requiring Defendants to disgorge all ill-gotten gains flowing from the conduct described in this Complaint;

5. For an award of attorneys' fees and costs of suit herein pursuant to Civil Code section 1798.84(g), Code of Civil Procedure section 1021.5, or as

otherwise allowable by applicable law;

6. For pre-judgment interest; and

7. For such other and further relief as the Court may deem just and proper.

DATED: May 26, 2015

Respectfully submitted,

BOUCHER LLP

By: /s/ Raymond P. Boucher

RAYMOND P. BOUCHER
SHEHNAZ M. BHUJWALA

Attorneys for Plaintiffs Kelly Tharp, Daniel Tharp, and Kenneth Coonce

BOUCHER LLP
21600 Oxnard Street, Suite 600
Woodland Hills, California 91367-4903

REQUEST FOR JURY TRIAL

Plaintiffs, individually and on behalf of a class of all others similarly situated ("Plaintiffs"), by and through their undersigned counsel of record, hereby respectfully requests a jury trial on all issues and counts so triable.

DATED: May 27, 2015

Respectfully submitted,

BOUCHER LLP

By: /s/ Raymond P. Boucher
RAYMOND P. BOUCHER
SHEHNAZ M. BHUJWALA

Attorneys for Plaintiffs Kelly Tharp, Daniel Tharp, and Kenneth Coonce